September 8, 2011

M. Keith Lipscomb, Esq.
LIPSCOMB, EISENBERG & BAKER, P.L.
2 South Biscayne Blvd.
Miami, FL 33131
Fax: (786) 431-2229

Re: Patrick Collins, Inc. v. Cox Communications Gulf Coast, LLC
(69.169.220.34, 5/1/11 1:21:40 UTC).

Dear Mr. Lipscomb:

Earlier this year, your firm filed a lawsuit, No. 2011-CA-3237, in a Jacksonville, Florida state court, which lacks subject-matter jurisdiction even to entertain copyright lawsuits,[1] relating to one or more motion pictures. In connection with said lawsuit, you served what purport to be subpoenas on one or more Internet service providers, asking for personal information involving some number of out-of-state subscribers. Subsequently, on or about August 18, 2011, one of the ISPs, Neustar (parent of Cox), sent a notification letter to a subscriber assigned the IP address 69.169.220.34, on or about May 1, 2011, at 1:21:40 UTC (the "Subscriber"), who is not and never has been a Florida resident, concerning the release of personally-identifiable information by

[1] See 28 U.S.C. § 1338(a) ("Such jurisdiction shall be exclusive of the courts of the states in . . . copyright cases.") (emphasis added); see also 17 U.S.C. § 512(h) (making clear that efforts to identify accused infringers belong solely in federal court, not state court); 17 U.S.C. § 301. Nor is a Florida court subpoena valid when addressed to a records custodian in Atlanta, Georgia.

Get a subpoena from the U.S. District Court for the Northern District of Georgia, or some other federal court that actually has authority over copyright matters, and then start again. See FED. R. CIV. P. 45(a)(2)(C), (b)(2)(B). By copy of this letter to Neustar/Cox, this ISP is being placed on notice that Neustar/Cox does not have authorization to disclose any information about the Subscriber. Further, all rights are reserved on the Subscriber's behalf, to proceed against Neustar/Cox for actual damages, liquidated damages, punitive damages, attorney fees, and other remedies provided by law under 47 U.S.C. § 551(f). Neither your subpoena nor any "order" purportedly obtained from a state court judge who obviously lacks subject-matter jurisdiction, provides any cover whatsoever to Neustar/Cox, against liability to customers, under 47 U.S.C. § 551(c). Neustar/Cox is therefore notified that it proceeds entirely at its own risk, and that the right to pursue class remedies also is reserved.

Neustar/Cox, pursuant to one of the pretext documents you served. The Subscriber has contacted this law firm, seeking representation.

The Subscriber did not distribute or copy the motion picture in question, nor did any member of Subscriber's household, nor any person authorized to use Subscriber's internet connection. The Subscriber respectfully declines to pay any money to your firm or your client because neither the Subscriber nor any member of his or her household did anything wrong or illegal.

The Subscriber is **not** one of your "John Does," and presently has no ability to assist you in any meaningful way, to ascertain the identity of any person allegedly making any alleged copy, as claimed in your lawsuit.

On behalf of the Subscriber, this letter is intended to serve two purposes. The first purpose is to extend a favor to you and your client, by saving everyone time and money. The second purpose is to serve as a reservation of rights, including but not limited to the Subscriber's rights under Rule 11 of the FEDERAL RULES OF CIVIL PROCEDURE, 28 U.S.C. § 1927, 17 U.S.C. §§ 504 and 505, other federal statutes, and state law in any applicable jurisdiction.

You and your client have a choice to make. On the one hand, you can let this one go, and focus your resources instead on other targets – presumably, those against whom you are able to present adequate evidence to prove actual copyright infringement.

This first approach makes sense precisely because the ISP subscriber in question never downloaded the movie in question, never infringed your client's copyright, and played no role in the alleged infringement (if any). From what we can determine, the likely[2] vector by which your contractor intercepted one or more "packets" of Internet traffic,[3] associated with the IP address listed above, would involve unauthorized third-party interception of service through a wireless node.

In this particular case, the wireless node in question, at the time your contractor recorded a "packet" on the Internet, was secured at best only with Wired Equivalent Privacy ("WEP")-level encryption, which would not have prevented unauthorized access from occurring. WEP, as you're

---

[2]Of course, we also cannot rule out the possibility, or even likelihood, that IP addresses intercepted by your contractor might have been "spoofed," by an unidentifiable third-party. This alternative would be a particularly likely explanation if your allegations are based on the interception of only a single "packet" of information.

[3]It is not clear from the information presently available to us, whether more than one "packet" allegedly was intercepted, involving the IP Address 69.143.2.241.

undoubtedly aware, is notoriously vulnerable. Tools such as aircrack-ng have been widely available for many years, that enable unauthorized persons to bypass WEP, and thereby gain access to wireless networks, with minimal effort, through an interface that is at least reasonably user-friendly.

The aircrack-ng Website, < http://www.aircrack-ng.org/ >, also boasts being able to crack WPA-PSK security on wireless networks. Accordingly, current state-of-the-art software tools enable both WEP and WPA encryption to be bypassed, reliably, with WEP subject to rapid cracking in a matter of seconds. See, e.g., *How to crack WEP Encrypted networks in seconds!*, THE LINUXG33K (Feb. 15, 2010), < http://linuxg33k.com/?p=45 >; Frederico Biancuzzi, *Gone in 120 Seconds: cracking Wi-fi Security*, THE REGISTER (May 15, 1997), < http://www.theregister.co.uk/2007/05/15/wep_crack_interview/ >; Andrew Nusca, *Researchers crack WPA Wi-Fi encryption in 60 seconds*, ZD Net (Aug. 27, 2009), < http://www.zdnet.com/blog/btl/researchers-crack-wpa-wi-fi-encryption-in-60-seconds/23384 >. That the availability of such tools is common knowledge in the technical community, and has been so for some time, is an understatement.

I'm not aware of anything in Title 17, let alone any other state or federal law, that prohibits the operation either of an unsecured wireless node, or one with security enabled that can be bypassed by even an amateur adversary.[4] Nor am I aware of any cognizable basis to impose copyright infringement liability vicariously on someone who did nothing more than operate a wireless node that happens to be vulnerable to unauthorized interception of service. Indeed, a movie company other than one of your clients has gone so far as to provide one of my clients with a complete release and covenant not to sue, as part of a zero-dollar final resolution, after learning that a vulnerable wireless node was at issue. If you have legal authority for the proposition that copyright or other liability can be premised on the mere operation of such a wireless node, which an unauthorized third-party has accessed without the user's knowledge or permission, then I'd be delighted to review it. Otherwise, we almost certainly can agree that my client did absolutely nothing wrong or illegal.

The alternative choice available to your client, of course, is to elect to drive up litigation expenses needlessly for both sides – in which case, it only stands to reason that the Subscriber reasonably would seek to be "made whole," for any and all burdens, financial and otherwise, that you voluntarily elect to impose on the Subscriber. For future reference, you are notified that the Subscriber intends to defend vigorously, and to seek any and all remedies that may be available, if

---

[4]MAC address filtering, as you've doubtless realized, is no solution because MAC addresses are easily spoofed. Indeed, such "spoofing" is trivial to accomplish with the right software tools installed. See, e.g., < http://en.wikipedia.org/wiki/MAC_spoofing >. The referenced Wikipedia article does not treat the subject comprehensively, and a myriad of other techniques can be discovered through a simple Google search for the right keywords.

you or your client elect to continue litigating. You are also reminded of the requirement in professional responsibility rules nationwide, that you and your firm are prohibited from communicating with the Subscriber, without my prior permission. See, e.g., FLA. R. PROF. CONDUCT 4-4.2.

We can predict with some confidence how the case will go, if you elect to run up everyone's bills. Two key issues would need to be addressed, in order to justify litigation beyond the "John Doe" stage – namely, personal jurisdiction and the merits. You and your client have the burden of proof on both of these topics, and mere guesswork, speculation, or subjective disbelief, cannot possibly constitute the sort of affirmative evidence that would be required to meet the threshold requirements to proceed any further against this putative defendant.

On the subject of personal jurisdiction, Keith, we're both familiar with the requirements of the Florida long-arm statute, and of the due process standard set forth in the Oldfield v. Pueblo De Bahia Lora, S.A., decision. The Subscriber does not have jurisdictional contacts with Florida sufficient either to trigger the operation of the long-arm statute, or to satisfy due process requirements. If you have evidence to the contrary, please feel free to share it with me and I'll be delighted to discuss with you what you think you have. In the meantime, it is our position that personal jurisdiction does not exist, and that any effort to seek either jurisdictional or identity discovery would represent nothing more than a bad-faith effort to multiply the burden and expense of litigation, vexatiously.

Concerning the merits, you are certainly aware that mere subjective disbelief of a subscriber's position, does not constitute evidence that in any way controverts the truth of what the subscriber is telling you. The threshold requirement, in order to get into court, actually requires evidence. If you have evidence to support an actual case of infringement against the Subscriber, personally, then I will be delighted to review what you think you have, and to discuss it with you. However, if you and your client elect to proceed based on nothing more than speculation, conjecture and wishful thinking, you do so entirely at your own risk, and the courts will be more than justified in making the Subscriber whole for any additional burden and expense that you elect to impose on him or her.

Thank you for your attention to these matters. All rights and remedies are reserved.

Very truly yours,

Eric C. Grimm

cc: The Subscriber
Neustar, Inc.
Cox Communications